NEW ZEALAND INSTITUTES OF TECHNOLOGY AND POLYTECHNIC QUALIFICATIONS IN INFORMATION & COMMUNICATIONS TECHNOLOGY

PRESCRIPTION: IE510 NETWORK OPERATING SYSTEMS

AIM OF MODULE:	To provide students with the knowledge and skills required to install, configure and maintain multi-user, multi-tasking network operating systems.
CREDITS:	14
STUDENT LEARNING HOURS:	140
CONTENT REVISED:	2004 (new)
PRESCRIPTION EXPIRY DATE:	Nov 2011
NOTE:	The content of this module is based on Cisco CNAP IT Essentials II, Ver 2.0 course content and will help prepare students for CompTIA's Server+ certification. When studied along with OS620 – Fundamentals of Unix, will help prepare students for CompTIA's Linux+ certification.

Level and Assessment Schedule

TOPICS	Highest Skill Level R	C	A	P	Suggested Assessment Percentage
1. Networked Operating Systems		*			5
2. Components of Common Network Architectures		*			10
3. TCP/IP networking		*			10
4. Network Services			*		10
5. Network Operating System Installation			*		50
6. Maintenance & Troubleshooting				*	10
7. Developing a Security Policy			*		5
					100

LEARNING OUTCOMES

The student will:

C	1.	Describe the basic origin, functions, and purpose of networked operating systems (NOS) including Windows and Linux.
C	2.	Describe the logical operation and physical components of common network architectures
C	3.	Describe TCP/IP networking, including origins, structure, and common protocols
A	4.	List the functions of various TCP/IP services and Directory Services, and connect network clients to appropriate servers
A	5.	Install NOS, including preparation, planning, configuration of hardware, network, services, and users, and demonstrate advanced NOS administration features
P	6.	Maintain and Trouble-shoot hardware and software, using a structured approach and variety of tools, including disaster recover techniques
A	7.	Describe a physical and logical security policy for a network

CONTENT

1. Networked Operation Systems

- A description of the basic origin, functions, and purpose of a Networked Operating Systems will include:
  - Overview of the basic components of an Operating System
  - Description of the components of a file system
  - Description of the history and functions of DOS and various versions of Windows
  - Description of the history and functions of Unix and Linux graphical and command line interfaces.
  - An overview of common network operating systems.

2. Components Of Common Network Architectures

- A description of the logical operation and physical components of common network architectures will include:
  - Brief summary of the benefits of networking, and types of network.
  - Description of characteristics of proprietary and open standards.
  - Detailed analysis of the OSI Reference Model, and open standards committees, including ISO, IEEE, ITU, EIA and ANSI.
  - Description of common network protocols, including TCP/IP, IPX/SPX, and Appletalk.

- Description of common LAN architectures, including Ethernet, Token Ring, and FDDI.
- Configuration of a Network card, including hardware settings, IP address, DHCP, and DNS.
- Description of network topologies, including bus, star, ring, mesh and hybrid.
- Description of network media types, including Coaxial and Twisted Pair cable, Fibre-optic cable, and Wireless Ethernet technologies.
- Description of network devices, including hubs, bridges, switches, and routers.
- Connection to the Internet, and the role of the ISP. Connection devices will include dial-up, DSL and cable modem.

3. TCP/IP networking

➢ A description of TCP/IP networking, including origins, structure, and common protocols will include:

- Description of the history of TCP/IP, including origins and rise in popularity, the TCP/IP model, IPv4 addressing structure and issues, subnetting.
- Description of the domain name system, how it interacts with the NOS, and WINS.
- Description of a variety of TCP/IP protocols from a server prospective. Protocols will include ARP, ICMP, TCP, UDP, DHCP, HTTP, FTP, Telnet, SMTP, POP3, IMAP.

4. Network Services

➢ An explanation of the functions of TCP/IP services and Directory Services will include:

- Description of the concept of a Network service, comparing the way services are described in Windows, Linux, and Netware.
- Description of the operation of remote administration and access services, including the use of those services for telecommuting, terminal emulation, telnet. Operation of the services will include configuration and access rights control.
- Outline interoperation of X.500, LDAP, Active Directory, eDirectory (NDS), NIS Directory Services. The components of Active Directory will be expanded, to include details of domains, Organizational Units, DNS, Domain Controllers, Replication, and Security.
- Configuration of a Linux machine as an NIS client.
- Consideration of NOS services from the client prospective. Services will include mail, printing, file sharing, web services such as FTP and HTTP, intranets, extranets, scripting, DNS, DHCP, domain services.

5. Network Operating System Installation

- Preparation for installation of a NOS will include analysis of the characteristics of a NOS. The analysis will include specific reference to history and distinctive characteristics of
  - various corporate Windows products.
  - Linux as a server NOS.

- Planning for the installation will include
  - Consideration of pre-installed Operating System.
  - Identification of hardware, and checking hardware and software compatibility.
  - Verification of network connectivity.

- Installation will include consideration of
  - Methods of installation, including advantages of using CD source and advantages of using network sources.
  - Determining appropriate BIOS Settings.
  - Requirements to start the installation program
  - Preparation of the hard disks, including planning and implementation of partitions, provision of swap files, and formatting.
  - Creation of initial administration accounts
  - Other choices to be made during installation.

- Configuration of the boot process will include
  - Outline of the process, including identification of required files, for Windows and Linux.
  - Detailed steps in the process, including interaction with the hardware BIOS functions.

- Consideration of problems which can occur in installation, including booting problems, those which arise during the installation process, and post-installation.

- Installation will follow prescribed steps for Windows and Linux server operating systems, and will include basic scripting, and configuration of services such as HTTP, FPT, Telnet, SMB, NFS, email, and printing.

- User Administration of the Linux server will include:
  - Consideration of the characteristics of the Linux login process.
  - Use of a Graphical interface, and a variety of Command Line shell interfaces.
  - Creation of a text file using a variety of commands in the vi editor.
  - Creation and management of users and groups in a Linux environment.
  - Basic management of the file system, including creating, and setting permissions, and mounting file systems.
  - Management and editing of configuration files, including description of runlevels, and system documentation.

- Explanation of the function of daemons, including how they can be started, stopped, and restarted. The explanation should include, a number of examples of installed services.

- Demonstration of advanced Network Operating System administration features will include:
  - Planning of backup strategies.
  - Installation and use of backup software, including automated backups.
  - Description of the various techniques used to map network drives in Linux, Windows, and Netware.
  - Management of partitions and processes in a Linux environment, including use of Cron jobs, and understanding a core dump, and setting the permissions for a process.
  - Monitoring of the critical resources of Disk, Memory, and CPU in Linux and Windows environment, including review of daily logs.
  - Analyzing and optimizing network performance starting form a baseline measurement, and using appropriate software.

- Installation and maintenance issues specific to Linux will be considered, including:
  - Description of a wide range of hardware concepts and terms, particularly the CPU and video systems.
  - Use of hardware diagnostic and management devices.
  - Sourcing of hardware drivers for Linux.

6. Maintenance & Troubleshooting

- A very wide range of techniques and tools will be described, based on a standard, simple, set of steps. Problem source will be isolated to one of these regions of the computer:
  - Hardware
  - Kernel
  - Application Software
  - User error

- A structured approach will be taken to troubleshooting, using a set of steps such as:
  - Gather information
  - Analyze the information
  - Formulate and implement a "treatment" plan
  - Test to verify the results of the treatment
  - Document everything

- Use will be made of system utilities and status tools to isolate the problem, including setserial, lpr, ifconfig, and route.

- Tools will be used to identify, stop, start, or restart, a process.

- Other techniques will be described, which address common problems, such as:

- Ways to deal with persistent problems.
- User of User Feedback, log files, or the dmesg command.
- Issues relating to boot problems, including recovery using emergency boot options
- Application package errors, including dependency issues, and failure of a package after it has been installed.
- Backup and restore errors.

➢ Troubleshooting network problems will include use of TCP/IP and Windows 2000 diagnostic tools.

➢ Disaster Recovery techniques will be explained, including:
- Risk Analysis, redundancy, clustering, scalability, and high availability
- Testing of the DR plan.
- Description of the concept of an alternative site for us in a disaster.

7. Describe a security policy

➢ A security policy for a network will be described, which includes provision for:
- An assessment of security needs.
- Policies for acceptable use, username and password security, network access rules, disposal of materials, virus protection, physical server room security, perimeter security, and use of removable media.
- Application of patches and updates in an appropriate manner.

➢ Online security sources will be consulted.

➢ The identification of threats and implementation of remedies for network security will be described.

➢ Common firewall scenarios will be described.

NOTES FOR TUTORS

A typical assessment strategy should include:
- practical skills tests
- laboratory exercises and worksheets
- group activities
- progressive on-line tests (CISCO Web Portal)
- summative (final) on-line test (CISCO Web Portal)
- kinaesthetic activities

LEARNING RESOURCES
- Cisco Networking Academy Program IT Essentials II:
  - Network Operating Systems Ver 2.0 Companion Guide
  - Network Operating Systems Ver 2.0 Lab Companion
  - Network Operating Systems Ver 2.0 Engineering Journal and Workbook
- Server+ Certification Bible. Trevor Kay. ISBN 0764548093